Rejections of Claims under Section 103

It is said in the Official Action that claims 26 and 27 are obvious over a combination of Aiello '307 and Aiello '928. The Siekierski patent is also considered herein.

Aiello's interest is in random numbers. The Aiello patents concentrate on a pseudorandom generator, and are entirely unrelated to gaming — but Applicant's invention, as originally presented, is strictly limited to gaming.

In view of the reversal in *Festo*, Applicant has now revised claim 26 to even more explicitly restrict the claims in this application to the gaming environment. This restriction, however, is apparent throughout Applicant's specification — beginning with the field of the invention and throughout the examination history of record.

With thanks to the Examiner for pointing out the discrepancy, the title of the application has now been revised to restore the original emphasis on gaming. This limitation also is a matter of File Wrapper Estoppel based on the comments of record.

As to Siekierski, Applicant's invention incorporates random number generation and cryptography technologies together, and applies them to the field of gaming. This THREE-WAY combination is not found in the cited art.

Siekierski has been cited to purportedly show a previous known relationship between random number generation and gaming, but it's only true that the Siekierski patent is entitled "Random Number Generating Techniques and Gaming Equipment Employing such Techniques". Actually, in substance Siekierski falls far short of teaching the kind of random-number usage that is specified in Applicant's claims 26 and 27.

More specifically, as both Aiello patents say (column 1, lines 49 through 51, emphasis added), "for complex methods and processes it is unlikely that the traditional generators will ever be proven to produce sufficiently random output". Siekierski's system is an example of just such a traditional system and is described in the following passage from Siekierski (column 3, lines 13 through 28, emphasis added).

> "In accordance with preferred embodiments of the present invention, a random number generator is provided which employs a white noise source to clock a counting arrangement whose maximum count exceeds the largest random number desired; a variable counter, clocked at a fixed rate, is loaded with random numbers obtained from said counting arrangement and each time said variable counter is counted down to a threshold state a new random number is read from said counting arrangement; random numbers obtained in this manner are then checked to ascertain their propriety and those which are accepted are then subject to pseudo-random number regenerative techniques to further randomize the same; random numbers obtained in this manner are then employed within a digitally controlled and operated gaming machine to select winning conditions."

Siekierski's system is thus based on just such a white-noise source. Such a source is conventionally a hardware device — not a cryptographically secure algorithm.

Hardware devices bear several fatal disadvantages as compared with cryptographically secure algorithms. Use of such hardware devices precludes application of deterministic algorithms, and such hardware sources are commonly subject to repetitive patterns, and almost always subject to spectral selectivity.

All this makes them dramatically inadequate in gaming. Neither Aiello nor Siekierski motivates the Applicant's claimed three-way combination — which is first motivated and first suggested only by the Applicant.

The remaining prior art also falls short of teaching the advanced association of deterministic-output based random number generation and cryptography belonging to Applicant's invention. This becomes immediately apparent as Siekierski opens (column 1, lines 43 through 51) with:

> "The provision of random numbers to a computer has typically been achieved through the storage of large tables of random numbers or by the provision of a random generator employing either hardware or pseudorandom number generation techniques. However, each of these techniques exhibits substantial drawbacks when applied to the development of gaming equipment or the like and frequently allow such equipment to be beaten by the skilled mathematician or the like."

Based on Siekierski's passage, pseudorandom number generators are beatable by the skilled mathematician — thus implying they do not use cryptographically secure random number generators such as DES (Data Encryption Standard) or AES (Advanced Encryption Standard) none of which has been beaten. Therefore they are not using cryptographic-quality or "strong encryption" numbers.

In contrast, cryptography is a central feature of Applicant's invention — and is specified in Applicant's claims. The present application at page 15, lines 8 through 20 describes and explains the preference for "a high quality, cryptographically strong pseudo-random number generator" as well as DES and international data encryption algorithm (IDEA) encryption circuits, while Fig. 7 of the application mirrors this preference with a signal-encryption step.

This is further emphasized in independent claim 26, which presently recites (emphasis added) —

> "A method for generating random numbers comprising the steps of . . . <u>encrypting</u> the signal; [and] grouping the <u>encrypted</u> signal into sets of raw pseudorandom numbers".

In summary, the invention as claimed represents an advanced integration of (1) cryptography, (2) deterministic-output-based random number generation, and (3) gaming — once again, a combination that is first seen in Applicant's invention and never before suggested.

The present invention is a great advance in the field of gaming. People of ordinary skill in the gaming business are traditionally unschooled in both computer sciences and crypto.

If it were obvious to combine Siekierski with Aiello to provide mathematically sophisticated gaming systems, since Siekierski has been available to the skilled artisan and inventing public for more than twenty years now, such combinations should be abundant in the art. None, however, has been made of record in this prosecution — and none is known to the Applicant.

In the Official Action, no prior art specifically combining these technologies has been introduced. This association, and the synergy it creates, are present in Applicant's invention only.

Applicant therefore respectfully submits that citation of the references in combination is hindsight, and this is prohibited by the patent law. The Applicant therefore respectfully asks that this rejection be withdrawn.

New claims 48 through 50

Applicant has now introduced four new claims that are believed to be within the elected subject matter. These claims

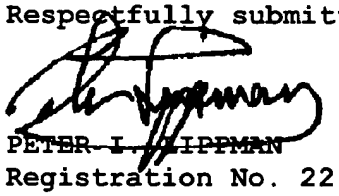
focus particularly on facets of that subject matter, chosen in the initial restriction, which complement claims 26 and 27.

Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully request the Examiner's favorable reconsideration and allowance of all the claims now standing in this case.

In addition, noting the extremely high cost of continuing prosecution of this application — not only to the Applicants but to the Government as well — it is earnestly requested that, should there appear any further obstacle to allowance of the claims herein, the Examiner telephone the undersigned attorney to try to resolve the obstacle.

Respectfully submitted,



PETER L. LIPPMAN
Registration No. 22,835
Attorney for the Applicants

Ashen & Lippman
4385 Ocean View Boulevard
Montrose, California 91020

TELEPHONE:
818/249-5961

October 1, 2002

AMENDED CLAIM

26. (twice amended) A method for generating random numbers for gaming; said method comprising the steps of:

providing a signal comprising a continuously changing deterministic output;

encrypting the signal;

grouping the encrypted signal into sets of raw pseudo[-]random numbers; [and]

verifying that the sets of raw pseudo[-]random numbers comprise independent, uniform, sets of statistically pseudo[-]random numbers; and

providing the verified sets to a gaming operation.